JOURNAL OF NUMBER THEORY 3, 13–18 (1971)

A Note on the Distribution of the Primitive Roots of a Prime

EMANUEL VEGH

Mathematics Research Center, U. S. Naval Research Laboratory, Washington, D. C. 20390

Communicated by S. Chowla

Received January 17, 1970

To my teacher Alfred Brauer on his 75th birthday.

In this paper it is shown that if $p = 4k + 1$ is a prime such that $\varphi(p-1)/(p-1) > 1/4$, then there is at least one pair of consecutive primitive roots modulo p. Generalization of this proposition, related results, and some computational work are also discussed.

1. INTRODUCTION

In this note we discuss questions concerning certain additive properties of the primitive roots, the quadratic residues and the quadratic nonresidues of a prime.

Let φ denote Euler's totient function. If p is a prime, let $g_1, g_2, \ldots, g_\lambda$, where $\lambda = \varphi(p-1)$, denote the primitive roots of p. If a is an integer, $(p \nmid a)$, then a' will denote a solution of the congruence $aa' \equiv 1 \pmod{p}$.

THEOREM 1. *If $p = 4k + 1$ is a prime such that $\varphi(p-1)/(p-1) > \frac{1}{4}$ and b is a quadratic residue modulo p, then there is at least one primitive root of p among the integers*

$$g_1 + b, g_2 + b, \ldots, g_\lambda + b, g_1 + b', g_2 + b', \ldots, g_\lambda + b'. \tag{1}$$

THEOREM 2. *If $p = 4k + 3 > 3$ is a prime such that $\varphi(p-1)/(p-1) > \frac{1}{3}$ and b is an integer $(p \nmid b)$, then there is at least one primitive root of p among the integers* (1).

For the special case when b is 1 (i.e., when we ask for pairs of consecutive primitive roots of a prime), Theorem 1 improves results recently obtained in [1]. The demonstration of these theorems suggests other elementary proofs for the following theorems of 0. Perron [2].

If p is a prime, let $n_1, n_2, \ldots, n_{(p-1)/2}$ (resp. $r_1, r_2, \ldots, r_{(p-1)/2}$) denote distinct quadratic nonresidues (quadratic residues) of p and let $r_0 \equiv 0 \pmod{p}$. We shall use the term nonresidue (residue) for quadratic nonresidue (quadratic residue). For convenience, we call r_0 a residue.

THEOREM 3 (Perron [2]). *If $p = 4k + 1$ is a prime then among the integers*

$$n_1 + a, n_2 + a, \ldots, n_{2k} + a \tag{2}$$

there are k residues and k nonresidues if a is a residue; $k + 1$ residues (including 0) and $k - 1$ nonresidues if a is a nonresidue.

THEOREM 4 (Perron [2]). *If $p = 4k + 1$ is a prime then among the integers*

$$r_0 + a, r_1 + a, \ldots, r_{2k} + a \tag{3}$$

there are $k + 1$ residues (including 0) and k nonresidues if a is a residue; k residues and $k + 1$ nonresidues if a is a nonresidue.

The method of proof for these results can also be used to prove similar results for primes of the form $4n + 3$.

2. PROOF OF THEOREMS 1 AND 2

Proof of Theorem 1. Let $p = 4k + 1$ be a prime such that $\varphi(p-1)/(p-1) > \frac{1}{4}$ and let a be an integer ($p \nmid a$). From the set of integers

$$g_1 + a, g_2 + a, \ldots, g_\lambda + a$$

select all the nonresidues and denote these, say, by

$$g_1 + a, g_2 + a, \ldots, g_n + a \qquad (n \leqslant \lambda). \tag{4}$$

Since -1 is a residue and $-g$ is a primitive root of p when g is, the integers

$$h_1 = -(g_1 + a), h_2 = -(g_2 + a), \ldots, h_n = -(g_n + a)$$

are nonresidues and

$$h_1 + a, h_2 + a, \ldots, h_n + a$$

are primitive roots of p. Naturally these n primitive roots belong to (2). The set (3) therefore contains the remaining $\lambda - n$ primitive root of p and no others. Since (3) contains k distinct nonresidues (this is proved independently in Theorem 4), the set (3) contains $k - (\lambda - n)$ distinct nonresidues which are not primitive roots of p.

If no member of (4) is a primitive root of p, then the n nonresidues of (4) together with the λ primitive roots of p and the $k - (\lambda - n)$ nonresidues of (3) which are not primitive roots of p, give a total of

$$\lambda + n + (k - (\lambda - n)) = 2n + (p - 1)/4$$

distinct nonresidues of p. Since there are exactly $(p - 1)/2$ nonresidues,

$$n \leqslant (p - 1)/8. \tag{5}$$

Let b be a residue and g a primitive root of p. g^{p-2} is also a primitive root of p, because $(p - 2, p - 1) = 1$. Since $b'g^{p-2}$ is a nonresidue, the congruence

$$b'g^{p-2}(g + b) \equiv g^{p-2} + b' \pmod{p}$$

implies that $g + b$ is a nonresidue if and only if $g^{p-2} + b'$ is a residue.[1]

If we consider the pair of numbers $g + b$ and $g^{p-2} + b' = h + b'$, as g runs through the $\varphi(p - 1)$ distinct primitive roots of p, and for each g select the nonresidue of the pair, we obtain sets of nonresidues

$$A = \{g_1 + b, g_2 + b, \ldots, g_n + b\}$$

and

$$A' = \{h_1 + b', h_2 + b', \ldots h_m + b'\}$$

where $g_1, g_2, \ldots, g_n$ (resp. $h_1, h_2, \ldots, h_m$) are distinct primitive roots of p, no two members of A (resp. no two members of A') are congruent, $n \geqslant 0$, $m \geqslant 0$, $n + m = \varphi(p - 1)$.

Without loss of generality we may assume that $m \leqslant n$ so that $\varphi(p - 1)/2 \leqslant n$. If no member of A is a primitive root of p, we have, using (5),

$$\varphi(p - 1)/2 \leqslant n \leqslant (p - 1)/8$$

or

$$\varphi(p - 1)/(p - 1) \leqslant \tfrac{1}{4},$$

a contradiction. Thus at least one member of (1) is a primitive root of p, and the theorem is proved.

[1] $g + b \not\equiv 0 \pmod{p}$, since g is a nonresidue and, for primes $p = 4n + 1$, $-b$ is a residue when b is a residue.

Proof of Theorem 2. Let $p = 4n + 3 > 3$ be a prime such that $\varphi(p-1)/(p-1) > \frac{1}{3}$, and let b be a residue of p. We construct sets of distinct nonresidues A and A' as in the proof of Theorem 1. In the present case we can only say that $n + m \geqslant \varphi(p-1) - 1$, since $g + b \equiv 0 \pmod{p}$ is possible, but only for at most one primitive root g.

Without loss of generality assume that $n \geqslant m$ so that $n \geqslant \varphi(p-1)/2$ when $p > 3$. If no member of A is a primitive root of p, then the $\varphi(p-1)$ primitive roots of p, together with the n distinct nonresidues of A, give rise to the inequality

$$\varphi(p-1) + \varphi(p-1)/2 \leqslant \varphi(p-1) + n \leqslant (p-1)/2,$$

or

$$\varphi(p-1)/(p-1) \leqslant \tfrac{1}{3},$$

a contradiction, Thus at least one member of (1) is a primitive root of p, when b is a residue,

If b^* is a nonresidue then $b = -b^*$ is a residue, since $p \equiv 3 \pmod 4$. Thus, as we have demonstrated, at least one of the integers of (1), say $g_1 + b = g_1 - b^* = h$, is a primitive root of p. Then $h + b^* = g_1$, and the theorem is proved.

3. Proof of Theorems 3 and 4

Let $p = 4k + 1$ be a prime and a an integer ($p \nmid a$). As shown by Perron, in order to prove Theorem 4, it is sufficient to prove Theorem 3 and observe that

$$r_0 + a, r_1 + a, \ldots, r_{2k} + a, n_1 + a, \ldots, n_{2k} + a \tag{6}$$

is a complete system of residues modulo p.

Proof of Theorem 3. Let a be a residue. If n is a nonresidue, then n', an', and $m = a^2n'$ are nonresidues.

The congruence

$$an'(n + a) \equiv m + a \pmod{p}$$

implies that $n + a$ is a residue if and only if $m + a$ is a nonresidue.[2] Therefore, for each nonresidue n there is a nonresidue m such that exactly one of $n + a$ and $m + a$ is a nonresidue. The set of integers (2) thus contains k residues and k nonresidues, when a is a residue.

[2] Here also $n + a$ and $m + a$ cannot be divisible by p, since each of n and m is a nonresidue and $-a$ is a residue.

Let a be a nonresidue. Then a' is a nonresidue and the integers

$$a'r_1, a'r_2, \ldots, a'r_{2k}$$

are distinct nonresidues. Then as we have just shown, there are k residues and k nonresidues among the integers

$$a'r_1 + 1, a'r_2 + 1, \ldots, a'r_{2k} + 1.$$

Multiplying each term of (7) by a and including $r_0 + a$ (a nonresidue) we obtain the set of integers

$$r_0 + a, r_1 + a, \ldots, r_{2k} + a, \tag{8}$$

which therefore consists of k residues and $k + 1$ nonresidues. By comparing (8) and (6), we see that (2) consists of $k + 1$ residues (including 0) and $k - 1$ nonresidues when a is a nonresidue. The proof is complete.

4. Remarks

Remark 1. It is natural to ask the following question. If p is a prime satisfying the conditions of Theorem 1 or Theorem 2 and a is an integer, does the set of integers

$$g_1 + a, g_2 + a, \ldots, g_\lambda + a \tag{9}$$

contain a primitive root of p?

We show that there are primes p and integers a for which no member of (9) is a primitive root.

Let $p = 13 = 4 \cdot 3 + 1$ so that $\varphi(12)/12 > 1/4$. The primitive roots of p are 2, 6, 7, and 11. If a is one of the nonresidues 6 or 11—note that $6' \equiv 11 \pmod{13}$—or the residue 3, then the integers (mod 13) in the set (9) are: 8, 12, 0 and 4; 0, 4, 5, and 9; 5, 9, 10, and 1, respectively. We have no primitive root of 13 in these sets. In fact, when $a = 6$, no member of (1) is a primitive root modulo 13.

Let $p = 11 = 4 \cdot 2 + 3$ so that $\varphi(10)/10 > 1/3$. The primitive roots of p are 2, 6, 7, and 8. If a is the residue 3 or the nonresidue 8, then the integers (mod 11) in the set (9) are: 5, 9, 10, and 0; 10, 3, 4, and 5, respectively. We again have no primitive root of 11 in these sets.

A direct computer calculation shows that the only primes $p < 2000$, for which there is an integer a such that no member of (9) is a primitive root of p, are $p = 2, 3, 5, 7, 11, 13, 31$, and 61.

Remark 2. Let $p = 4k + 3$ be a prime such that $\varphi(p-1)/(p-1) > 1/3$ and a an integer such ind $a \equiv 0 \pmod{q_1 q_2 \cdots q_s}$, where q_i run through all the odd prime divisors of $p - 1$ or through all prime divisors of $p - 1$. We show here that at least one member of (9) is a primitive root of p.

By Theorem 2 at least one member of (1) is a primitive root of p, say $g_1 + a'$. Then

$$a^2(g_1 + a') \equiv a^2 g_1 + a \pmod{p}.$$

It is obvious that

$$(\text{ind } a^2(g_1 + a'), p - 1) = (\text{ind } a^2 g_1, p - 1) = 1,$$

so $a^2 g_1$ and $a^2 g_1 + a$ are primitive roots of p.

A similar result may be proved for primes of the form $4k + 1$.

ACKNOWLEDGMENT

The author wishes to thank Miss Janet Fisher for writing the computer program mentioned in connection with Remark 1.

REFERENCES

1. E. VEGH, Pairs of consecutive primitive roots modulo a prime, *Proc. Amer. Math. Soc.* **19** (1968), 1169–1170.
2. PERRON, O. Bemerkung über die Verteilung der quadratischen Reste, *Math. Z.* **56** (1952), 122–130.